NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Inherent Risk Assessment Guide

October 2014

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

This Inherent Risk Assessment (IRA) Guide (the "Guide") describes the process Compliance Enforcement Authorities (CEAs) use to assess inherent risk of registered entities and serves as a common approach for the North American Electric Reliability Corporation (NERC) and the eight Regional Entities (REs) for implementing and performing an IRA.

CEAs[1] perform an IRA of registered entities to identify areas of focus and the level of effort needed to monitor compliance with enforceable NERC Reliability Standards (Reliability Standards). The IRA is a review of potential risks posed by an individual registered entity to the reliability of the bulk power system (BPS). An assessment of BPS reliability impact due to inherent risk requires identification and aggregation of individual risk factors related to each registered entity, and the consideration of the significance of BPS reliability impact for identified risks. An IRA considers risk factors such as assets, systems, geography, interconnectivity, prior compliance history, and overall unique entity composition when determining the compliance oversight plan for a registered entity. CEAs will perform the IRA on a periodic basis, with the frequency based on a variety of factors including, but not limited to, changes to a registered entity, significant changes to reliability risks, or emergence of new reliability risks. This IRA Guide provides a framework for performing each phase of the IRA and identifies expected outcomes.

Appendix A contains definitions of terms used within the Guide.

Revision History

Date	Comments
July 16, 2014	Posted for Board of Trustees Policy Input
October 10, 2014	Posted for 2015 Implementation

[1] NERC ROP, Section 401 (Scope of the NERC Compliance Monitoring and Enforcement Program): CEAs, which consist of NERC and the eight Regional Entities, carry out Compliance Monitoring and Enforcement Program (CMEP) activities in accordance with the NERC ROP and Appendix 4C CMEP, the respective Regional Delegation Agreements between NERC and each RE, and other agreements with the Canadian and Mexican regulatory authorities.

1.0 IRA Introduction

1.1 IRA Role within the Overall Risk-Based Compliance Oversight Framework

CEAs use the IRA as a process within the Risk-Based Compliance Oversight Framework (Framework) as a key input into development of each compliance oversight plan for a registered entity. The IRA considers outputs from the risk elements (see section 1.2.1 for more details). IRA results are key input sources to the Internal Controls Evaluation (ICE), if used, and in determining an overall compliance oversight plan for a registered entity. Figure 1 below Illustrates the role of IRA within the Framework.

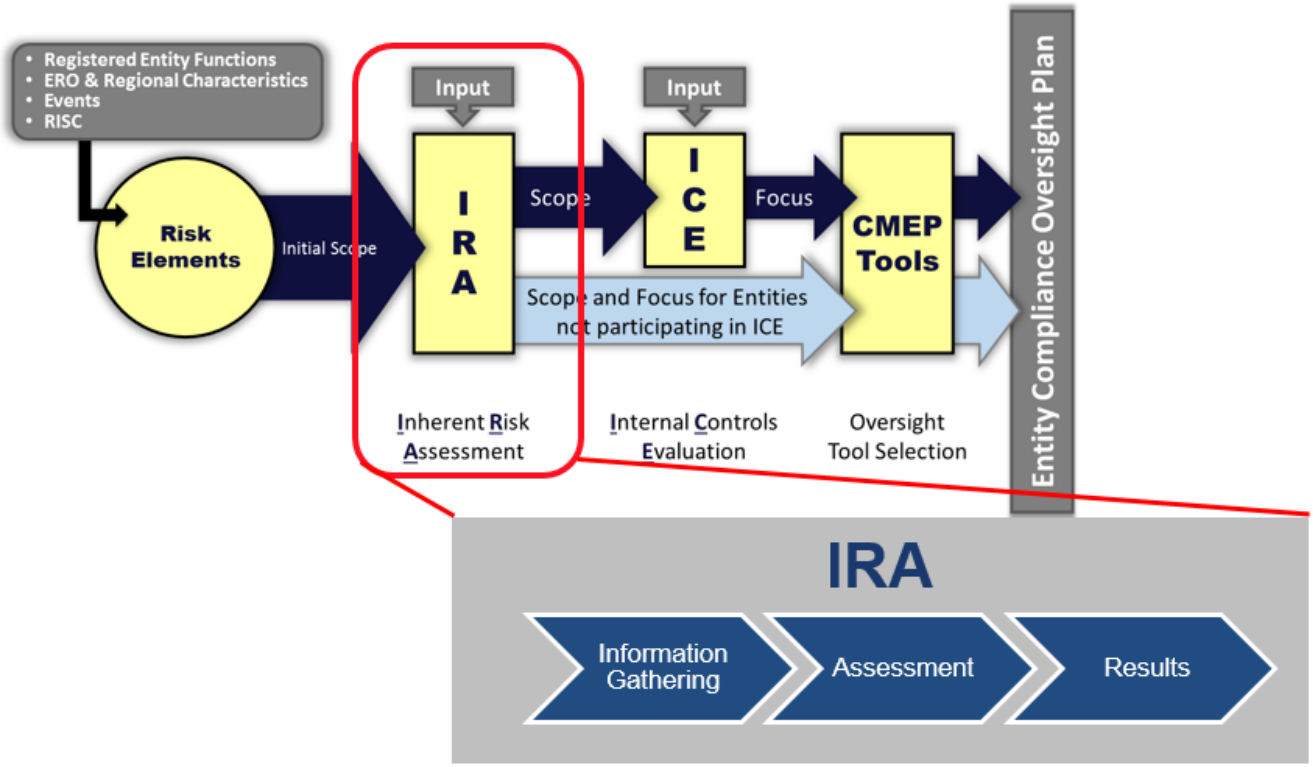

Figure 1. Risk-based Compliance Oversight Framework

The IRA is based on an entity's unique inherent risks to the reliability of the BPS. The IRA guides CEAs in identifying risks and determining areas of focus for a specific registered entity. The IRA process will also identify specific Reliability Standards and Requirements that the CEA should consider for compliance oversight.

1.2 Major inputs into the IRA

1.2.1 Risk Element Inputs

The ERO Enterprise assesses risks to the reliability of the BPS, as well as mitigating factors that may reduce or eliminate a given reliability risk. The ERO Enterprise developed a Risk Elements Guide that describes the process for identifying risks to the BPS and maps associated registration functional categories and Reliability Standards to those risks.

CEAs should use the annual ERO CMEP Implementation Plan, including the Regional Implementation Plans, as input into the IRA. The ERO CMEP Implementation Plan identifies specific:

- ERO Enterprise risks to the reliability of the BPS for compliance monitoring.
- Associated Reliability Standards and Requirements mapped to the reliability risks.
- Regional risk considerations.

Refer to the Risk Elements Guide and the annual ERO CMEP Implementation Plans for further details.

1.2.2 Understanding the Registered Entity

Understanding a registered entity is an essential aspect of the IRA and of the Framework. A CEA should conduct activities to gain an understanding of the registered entity and its operations (e.g. geographical foot print, prior compliance history/performance, types of BPS assets, recent asset acquisitions/changes, etc.). Some activities for understanding the registered entity and its operational environment are described below.

2.0 IRA Process

The IRA process involves:

- Gathering and maintaining registered entity specific information and data (e.g., past performance, historical registered entity information on file within CEA Entity databases).
- Proactively identifying risk trends and prevalent practices at the registered entity.
- Establishing qualitative and quantitative risk factors for evaluating whether areas and levels of oversight focus is appropriate.
- Considering the applicability and significance of standards / requirements that may apply to an entity based on the assets they own or operate.
- Identifying areas where special consideration may be necessary. Some examples include (1) changes to the entity's asset composition, (2) unique power system configuration or unique organizational structure, or (3) significant system events.
- Understanding a registered entity's internal environment, including the tone of the organization and compliance environment for compliance with Reliability Standards.

The CEA should gather and review information about a particular registered entity for appropriateness (relevance) and sufficiency (completeness and accuracy) to afford a reasonable basis for a conclusion. During this process, the CEA should leverage knowledgeable parties, both internal and external, to provide input as necessary. Professional judgment should be applied during the process and documented to support the conclusions reached. The IRA output should be used as a key input when developing the compliance oversight plan for a registered entity. Figure 2 below illustrates the overall IRA process.

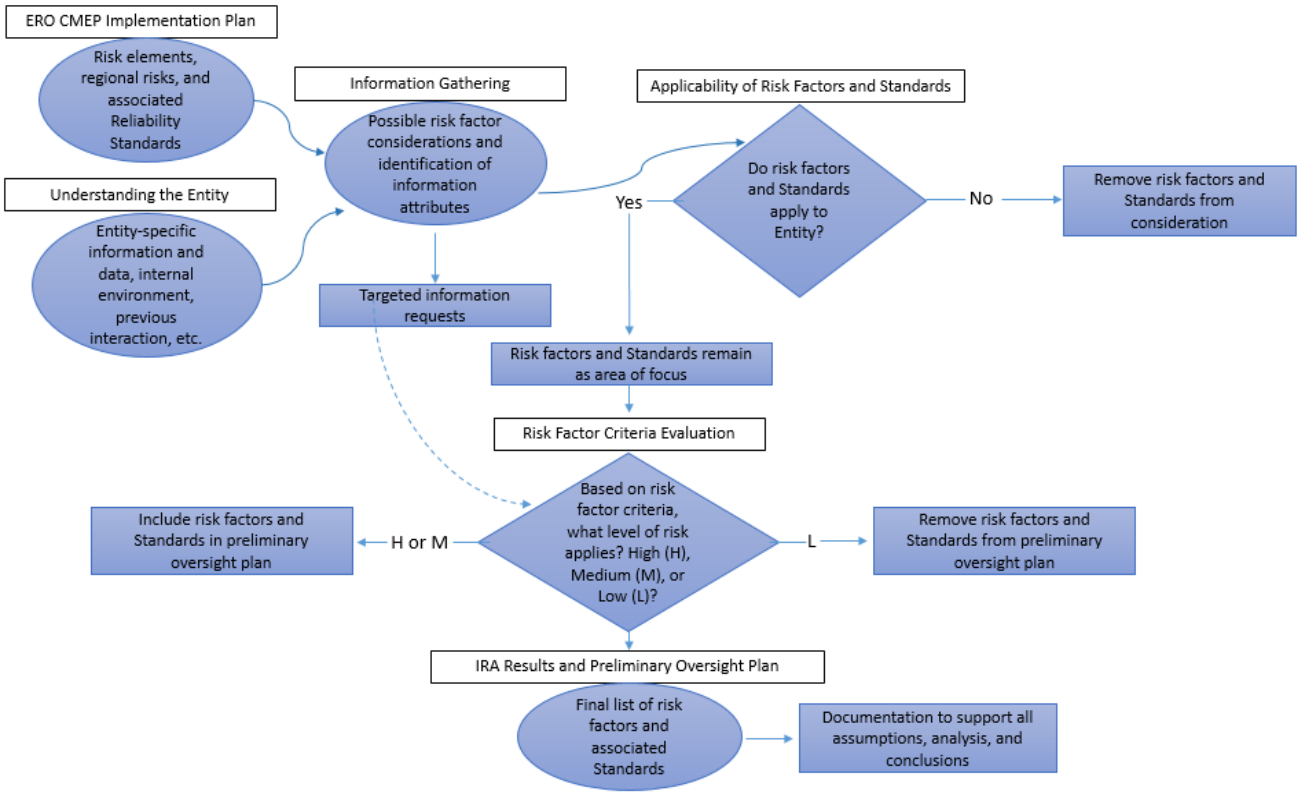

Figure 2. IRA Process Flow Chart

2.1 Information Gathering

Guidance is provided for the following elements of this phase:

- Procedures the CEAs should follow to identify, collect and analyze information
- Outcomes of the Information Gathering phase

2.1.1 Information Gathering Process

2.1.1.1 Key Inputs (Sources):

- Prioritized list of known risks to the reliability of the BPS and associated Reliability Standards and Requirements (ERO CMEP Implementation Plan)
- Understanding of the registered entity and its operations (Understanding the Registered Entity section and IRA process steps herein)
- Information Attributes Lists and their common sources (Appendix B)
- Possible Risk Factor considerations (Appendix C)

2.1.1.2 Gather ERO Enterprise and Regional Risk Focus Areas

The first step is to gather information pertaining to the potential BPS reliability risks and the associated Reliability Standards and Requirements for the registered entity's functional registration(s).

2.1.1.3 Determine entity specific information needs to perform IRA

The CEAs should inventory registered entity information available at both NERC and the Regional levels to identify (1) the current information on file, (2) any information requiring updates or revisions, and (3) any incomplete information. The following steps may assist the CEAs in identifying the information already available, while highlighting additional information that may be required to complete the information lists for IRA decision making:

- Review outputs from the Risk Elements Guide and annual CMEP Implementation Plan for applicability to the entity (i.e., Do certain known risks to the reliability of the BPS, based on functional registration, apply to the entity and drive the need for further information?) (See Section 2.2.1 herein for further details on Risk Elements outputs). Leverage the CEA's existing understanding of the entity which may include inventorying and aggregating information already held by the ERO (e.g., information from prior audits, compliance history information, and Transmission Availability Data System (TADS) information, etc.). Reconcile the information on hand with the information attributes list in Appendix B to identify potential information gaps and data verification needs (See Section 2.2.2 herein for detail on understanding the entity). The information attributes list in Appendix B contains possible information for CEAs to consider during the IRA process.
- Reconcile and update, as necessary, risks factors to Reliability Standards and Requirements, and information on hand to identify further data needs for decision making in Section 2.2. The risk factors applied to the entity can be used to identify further information requests. Refer to Appendix C for examples of risk factors and risk factor criteria. CEAs should consider the context of a registered entity's size, location, or function in applying or developing risk factors and risk factor criteria such as those examples listed in Appendix C.

2.1.1.4 Develop Targeted Information Request List

After completing an inventory of the information that is readily available and identifying the additional information needs, the CEA may develop targeted information requests. The information attributes list should be used as a resource when developing the information request. Refer to Appendix B for further instructions on information gathering and information attributes used during the Information Gathering phase.

The CEA should minimize its request for IRA information from registered entities when the same information is available within the ERO or through other reliable sources. The CEA should confirm information collected is both appropriate and sufficient, noting that appropriateness is a measure of the quality of information that encompasses its relevance, validity, and reliability whereas sufficiency is a measure of the quantity of information that is necessary to draw conclusions.

For example, to verify information appropriateness, CEA may confirm the accuracy and reliability of facility data with other independent sources such as maps, prior data requests, reliability assessments, event reports, and information from the Planning Authority (PA) or Transmission Planner (TP). Additionally, the information provided by the PA or TP should have a sufficient level of detail so one can understand the entity's area of operations (maps, facilities, neighboring systems, etc.)

The CEAs should tailor information requests based on the following:

- Outputs from risk elements(see Section 2.2.1 for further details)
- Understanding of the entity (see Section 2.2.2 for further details)
- Risk factors, as referenced in Appendix C, and associated Reliability Standards and Requirements (preliminary list)

The CEAs should exercise professional judgment when identifying the most reliable sources that will provide the required information to perform an IRA. Professional judgment requires an appropriate skill set and experience to conduct the IRA. If comfort can be obtained that it is accurate and complete, CEA staff should use existing information to conduct the IRA, rather than creating new data requests to the registered entity. Any additional data requests should be germane to the IRA.

Key Questions in Information Gathering Phase

2.1.1.2

- What ERO Enterprise and Regional Entity risks, and associated standards and requirements, are applicable to the functional registration of the registered entity?

2.1.1.3

- What risk factors are in scope?
- What registered entity specific information do we need?

2.1.1.4

- Where do we get information from?
- Is the information appropriate and sufficient?

2.1.2 Key Outputs

- Known risk to the reliability of the BPS and associated Reliability Standards and Requirements from risk elements that are applicable to the registered functions of the registered entity.
- Preliminary list of risk factors applicable to the registered entity
- Updated / verified registered entity data

- Targeted Information Request List

2.2 Assessment

Guidance is provided for the following elements of this phase:

- Identify processes the CEAs should follow to assess and draw conclusions around risk elements output, risk factors, and Reliability Standards and Requirements applicable to the registered entity.
- Identify outcomes of the Decision Making phase.

2.2.1 Assessment Process

2.2.1.1 Key Inputs (Sources):

- Prioritized list of known risks to the reliability of the BPS and associated Reliability Standards and Requirements (Risk Elements and Region-specific risks identified in annual CMEP Implementation Plan) Preliminary list of applicable risk factors (section 2.1 Information Gathering)
- Risk Factor Examples (IRA Appendix C)
- Updated / verified registered entity data (section 2.1 Information Gathering)

2.2.1.2 Risk Factor and Reliability Standards and Requirements Applicability Review

The purpose of this step is to review information gathered to confirm the applicability of Reliability Standards and Requirements to the registered entity. The initial list of potentially applicable Reliability Standards and Requirements is determined based on a registered entity's functional designation[2]; however, because of specific characteristics of a registered entity (e.g. certain types of assets are not owned or operated by them) a number of Reliability Standards and Requirements may not be applicable to them (see examples below). The CEA should use information gathered and risk factors to exclude the registered entity's non-applicable Reliability Standards and Requirements.

The CEA should document conclusions reached for Reliability Standards and Requirements excluded from further analysis based on the Applicability Review. For all Reliability Standards and Requirements (as well as corresponding risk factors) that are deemed applicable, the CEA will complete the Risk Factor Analysis in Section 2.2.1.3.

To illustrate the Applicability Review, refer to the example below. Using collected registered entity information, the CEA will first determine whether or not certain risk factors and associated Reliability Standards and Requirements are applicable to the registered entity.

Example: Applicability of Certain Risk Factors and Reliability Standards and Requirements

***Risk factor*:** Under Voltage Load Shedding (UVLS) consideration

Information Attribute: Entity has automated UVLS and stated that it recently utilized UVLS

***Standard and Requirement Considerations*:** EOP-003-2 R2

[2] An entity's functional designation is based on the nature of the entity which includes, for example: (1) balancing authorities, (2) distribution providers, (3) generator operators, (4) generator owners, (5) reliability coordinators, (6) transmission operators, and (7) transmission owners.

Decision criteria: Does the information collected indicate an applicable risk factor that should be considered in further analysis?

Applicability Review and Conclusion: Yes, the entity indicated it recently utilized its automated UVLS. Therefore, the CEA should further evaluate the risk factor and apply criteria to determine the depth of focus for this risk factor.

Note: The example above is for illustrative purposes only. When making the determination of what would be applicable to a specific registered entity, the CEA will need to identify all relevant risk factors and associated Reliability Standards and Requirements based on the information gathered.

2.2.1.3 Risk Factor Analysis

After performing the Applicability Review, the CEA reviews the collected entity-specific information, as well as other known risks to the reliability of the BPS (i.e., inputs from Risk Elements as reflected in the CMEP IP), to determine areas of focus within the registered entity. Risk factors associated with the registered entity are weighted based on risk factor evaluation criteria as shown by the criteria columns in the Appendix C – Risk Factor Examples.

The CEA should reconfirm the Reliability Standards and Requirements that are applicable to the registered entity's function. For example, risk factors associated with special protective systems (SPSs) do not apply to a Transmission Operator (TOP) that does not have SPSs within its footprint. Additionally, a Vegetation Management risk element may not present a high risk to an entity operating in the desert in the Southwest if the entity operates in a climate with no or very limited vegetation that can affect transmission lines. Once the CEA reconfirms the Reliability Standards and Requirements applicable to the registered entity, based on the defined risk factor evaluation criteria, it will assess the risk factors applicable to the registered entity and determine the level of risk associated with each risk factor.

Refer to Appendix C for a list of risk factors and risk factor criteria that can be used as a guide when determining an entity's unique inherent risks to the reliability of the BPS. Although Appendix C can assist in evaluating the criteria of applied risk factors, consideration must be made for a registered entity's size or function. The relative importance of a particular risk -factor criterion may need to be evaluated compared to a registered entity's size or function.

Certain risk factors and the associated criteria/thresholds may vary by region, by entity size, or by function. Depending on the unique characteristics of the entity, the conclusion may be that some of the listed risk factors may be more applicable or contributory than others, some may not be applicable at all, or there may be additional risk factors not listed that would be appropriate to consider. For example, while certain characteristics of a registered entity may result in a higher assignment of risk relative to a specific risk factor, the registered entity's size or function may mean that the risk factor itself does not merit significant consideration in determining an entity's unique inherent risks to the reliability of the BPS. This also reflects the notion that some risk factors that one might associate as contributory towards determining overall inherent risk of an entity for a larger entity may contribute differently to the evaluation of a smaller entity. The CEA should document their professional judgment used in identifying risk factors and developing risk factor evaluation criteria.

To illustrate the risk factor analysis, refer to the example below:

Example: Risk Factor Analysis for a GOP

***Registered function*:** GOP

***Risk factors*:** UVLS and System events and trends

***Associated Reliability Standards & Requirements*:** VAR-002-2b R1, R2, R3, R4

***Information Attributes*:**

- Reportable events history (voltage instability/UVLS load shed events)
- Generating Availability Data System (GADS), Transmission Availability Data System (TADS) data mining
- Presence of reactive compensation devices
- Prior compliance history

Risk Factor Criteria:

- High – urban area or critical customers without any other nearby generators that can provide voltage support and inadequate compensation devices in the area. Or regions served by multiple transmission lines from outside the local area, where special measures must be taken to schedule sufficient local generation to support voltage in the area.
- Medium – same conditions as above but with ample compensating devices and UVLS installations.
- Low – voltage sensitive areas with multiple nearby generators that can provide MVAs.

Analysis and conclusion:
The CEA applies professional judgment and reaches conclusions based on the assessment of information attributes reviewed against the defined risk factor criteria. Qualitative and quantitative attributes associated with the information should indicate whether the risk factor is high, medium, and low.

The risk factors and associated Requirements under VAR-002-2b R1, R2, R3, R4 would remain in scope if the CEA determined that the entity's characteristics meet higher ranked criteria.

2.2.1.4 Quality Review of IRA conclusions:

The CEA should leverage subject matter experts throughout the IRA process as needed. Once preliminary conclusions about the applicability of risk factors and Reliability Standards and Requirements have been reached, the CEA should consider the findings of other subject matter experts (if applicable) or conduct an independent management review of the IRA output to verify they appear appropriate based on the information known about the registered entity.

2.2.2 Key Outputs

- Updated list of risk factors used to assess the registered entity's inherent risk to the reliability of the BPS.
- Comprehensive list of Reliability Standards and Requirements that are determined to be applicable to the registered entity based on the inherent risks to the reliability of the BPS.
- List of risk factors and criteria (including evaluation of impact) mapped to applicable Reliability Standards and Requirements.
- Documentation supporting inclusion/exclusion of Reliability Standards and Requirements.

Key Questions for Decision Making Phase

2.2.1.1

- Based on Requirement and registered entity data,
  - Which Reliability Standards and Requirements are not applicable?
  - Which risk factors are not applicable?

2.2.1.2

- Which risk factors are used to assess the level of significance of Reliability Standards and Requirements in scope?

2.2.2

- What are the areas of focus?
- What level of effort should be assigned to each area of focus?
- What is our preliminary compliance oversight plan?

2.3 Results

Once the IRA decisions process is complete, CEAs should document assumptions made, the specific information leveraged to identify areas of focus, and level of effort that occurred to perform the IRA. Additionally, the IRA process should facilitate a collaborative dialogue with the registered entity regarding applicable risks.

2.3.1 Results Process

CEAs should document each phase of the IRA process. To document each IRA phase, Information Gathering, Decision Making, and IRA Outcomes, CEAs should:

- Identify processes the CEAs should follow to document conclusions around risk factors, Reliability Standards and Requirements applicable to the registered entity.
- Document the outcomes of the Decision Making phase

2.3.2 Key Outputs

- Identification of the inherent risks to the reliability of the BPS that are applicable to the registered entity
- List of the associated Reliability Standards and Requirements that could help prevent the inherent risks applicable to the registered entity
- Summary of how the IRA ties to the different analyses performed and subsequent conclusions
- Draft compliance oversight plan for the registered entity

Key Questions for IRA Outcomes Phase

2.3

- What was done to support the conclusion?
- What level of information should the compliance oversight plan include?
- How is supporting information documented and maintained?

2.4 Sharing IRA Results with the Registered Entity

CEAs should facilitate a collaborative dialogue with the registered entity throughout the IRA process. As needed, CEAs may work with the registered entity to ensure the CEA has appropriate and sufficient information to conduct the IRA and reach accurate conclusions. After the CEA finalizes IRA results, the CEA should share the summary results with the registered entity (including risk areas and impact on the scope of monitoring).

CEAs are owners of the IRA process and CEAs are ultimately responsible for assessing inherent risks and potential risks to reliability posed by a registered entity.

2.5 Frequency and Revision of Inherent Risk Assessment

The IRA will be performed on a periodic basis, with the frequency based on a variety of factors including, but not limited to, changes to a registered entity and significant changes or emergence of new reliability risks.

CEAs can review and revise the IRA of a registered entity at any time and should be cognizant of the effect that a registered entity's risks may pose to maintaining a reliable BPS. This understanding is essential in performing an IRA, as it establishes a frame of reference by which the IRA is conducted. Importantly, an IRA may need to be revised as new, emerging, or unique information is obtained either about the registered entity or about risks to the reliability of the BPS. Some activities that occur and drive an IRA revision may include a system event, change in compliance history or activity, significant change to organization structure, changes to Reliability Standards, etc. For example, if a registered entity's current IRA is based on ownership of a specific asset, but the registered entity later sells or retires that asset, the CEA should revise the IRA to consider the asset ownership change. Similarly, if an event occurs that highlights a never-before-considered reliability risk, the CEA should consider whether it needs to revisit an IRA to determine how the new reliability risk impacts a registered entity.

2.6 IRA Feedback into ERO Enterprise Processes

An ERO Enterprise feedback loop involving compliance monitoring activities will help inform future priorities, projects in the NERC standards development process, and other ERO Enterprise program areas. As CEAs conduct IRAs, CEAs may identify certain risk focus areas that do not map to current, enforceable Reliability Standards. The CEAs may also determine other gaps, revisions, or retirement needs of Reliability Standards or other program activities. That feedback loop will mature with more experience implementing risk-based compliance monitoring methods.

3.0 IRA Documentation

3.1 Results Documentation

The CEAs should follow established documentation protocols, refer to the NERC Rules of Procedure, and use its professional judgment, where appropriate, when determining documentation needs throughout the IRA process. The CEA should maintain documentation that clearly supports conclusions made around oversight scope. Documentation includes all data and information obtained, reviewed, and used as inputs to the IRA, and should be linked to conclusions so that one can easily see why final determinations were made. The CEAs should maintain documentation, demonstrating the nature and extent of information reviewed and IRA conclusions reached.

The extent of the resulting documentation is directly linked to the (1) nature, size, and complexity of the issues, (2) procedures performed, and (3) methodologies and technologies used during the process. The more significant and complex these factors are, the greater and more detailed the documentation may be.

3.2 Documentation Retention

Upon completion of the IRA process, the CEA should retain relevant documentation that supports the procedures performed and conclusions reached. Examples of documentation that should be retained includes, but is not be limited to, the following: IRA programs, analyses, memoranda, summaries of significant findings or issues, checklists, abstracts, copies of important documents, and paper or electronic correspondence concerning significant findings or issues. Additionally, finalized narrative descriptions, questionnaires, checklists, and flowcharts created through the IRA process are also considered important documentation and should be retained.

When making the determination of the nature and extent of documentation that should be retained, the CEA should consider the information that would be required for an experienced compliance team member to understand the work performed and the conclusions reached during the IRA. Incomplete or preliminary documentation does not need to be maintained.

4.0 References

Below are a list of reference materials that support the basic principles, concepts, and approaches within this Guide. The CEAs can use these reference materials to assist in applying the IRA process detailed in this Guide. These reference materials can assist with determining: (1) where and to what extent professional judgment should be applied, (2) the sufficiency and appropriateness of evidence to be examined, and (3) the sufficiency and appropriateness of the documentation required.

- Generally Accepted Government Auditing Standards (GAGAS), located at: http://gao.gov/assets/590/587281.pdf
- ERO Compliance Auditor Handbook, located at: http://www.nerc.com/pa/comp/Pages/ERO-Enterprise-Compliance-Auditor-Manual.aspx
- Annual ERO CMEP Implementation Plan, located at: http://www.nerc.com/pa/comp/Resources/Pages/default.aspx
- NERC Rules of Procedure (ROP), located at: http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx

Appendix A – Definitions

Areas of Focus: The outcomes of the IRA process and determines: Risks deemed applicable to the registered entity; Reliability Standards deemed appropriate to apply to the registered entity; and mapping of risk factors to Reliability Standards and Requirements

Compliance Oversight Plan: A plan consisting of the oversight strategy for a registered entity. The plan will usually include areas of focus, level of efforts, timing, and overall strategy on use of CMEP tool(s).

Compliance Enforcement Authority: NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the Reliability Standards.

CMEP Tools: In context of IRA, these are tools used during the compliance monitoring processes to develop the CEAs' Compliance Oversight Plan. CMEP tools are described in Section 3.0 of the NERC Rules of Procedure, Appendix 4C, and includes but are not necessarily limited to Compliance Audits, Spot Checks, Self-Certifications, and Periodic Data Submittals.

Information Attributes: Registered entity-specific data or information that is collected by Regional Entities to be used during IRA and the related process to support development of Compliance Oversight Plan.

Inherent Risk: Risks specific to a registered entity that could impact the reliability of the BPS.

Inherent Risk Assessment: A review of potential risks posed by an individual registered entity to the reliability of the BPS.

Preliminary Area of Focus: At any point during the IRA phases, the preliminary list of risks and mapped Reliability Standards that have not been removed from the potential Area of Focus.

Professional Judgment[3]: Represents the exercising of reasonable care and professional skepticism. Reasonable care concerns acting diligently in accordance with applicable professional standards and ethical principles. Professional skepticism is an attitude that includes a questioning mind and a critical assessment of evidence.

Reasonable Assurance[4]: Conclusions based on evidence that is sufficient and appropriate to support the CEA's conclusions. (Note: Emphasis on reasonable, not 'complete' or 'absolute' assurance).

Risk: A possibility of an event occurring that will have an impact to the reliability of the BPS.

Risk-based Compliance Oversight Framework: The Compliance Oversight Framework is the risk-based approached that includes process steps and considerations of Risk Elements, IRA, Internal Control Evaluation (ICE), and CMEP Tools.

Risk Factors: Considerations used during an IRA to identify a registered entity's risk characteristics that are inherent to a registered entity's configuration and may impact the reliability of the BPS.

[3] Generally Accepted Government Auditing Standards Section 3.61.

[4] Generally Accepted Government Auditing Standards Section 6.03.

Appendix B – Information Attribute List

The information attribute list below contains examples of information that is to be considered during the IRA process. The information attribute list is the list of information that should be considered during the IRA process regardless of the analytic tools, techniques, or methods applied for risk identification. The information attribute list is not intended to be an all-inclusive list for information considerations, but should serve as a guide to identify information needed for an IRA.

The information attributes list summarizes the purpose of each information attribute, as well as provides criteria to understand data standards and rationale for collection. Specifically, the data criterion considers the nature and criticality of the data when conducting an IRA. It should be leveraged as a guide for identifying relevant data to be collected, but is not a comprehensive list.

There are various sources of information used to collect data. These sources include: publicly available sources, third-party sources, CEA internal sources (i.e., NERC and Regional Entities), and direct information gathering from the registered entity. This guidance recognizes that each Regional Entity may need to identify and prioritize its own methods for collecting information attributes based on its individual resources and capabilities.

The CEA can refer to the "source" descriptions for each information attribute for possible collection methods. NERC advises Regional Entities to collaborate, where possible, to obtain registered entity information. However, due to certain limitations, a Regional Entity may have to contact the registered entity directly.

Information Attribute Examples			
Information Attribute	**Subcategory of Information**	**Purpose of Information Attribute**	**Possible Source(s)**
Total megawatt capability	Peak Load and area capacity	Magnitude of possible impact for BAs/TOPs/LSEs	Reliability Assessment Subcommittee (RAS), TP/PA models, Entity
Interconnection points and key facilities and paths	Cranking paths, Next start paths, synchronization points, and BA boundaries	Understanding of potential operating risk for certain Entity's facilities.	Regional assessments, TP/PA models, tieline database, one lines (Entity), RC/TOP information, critical asset list (Region or Entity), PRC-023 list
Special Protection Systems	Design information	Reflects potential risks in system, management, awareness. Misoperation occurs if not working when called upon and understanding of roles and responsibilities(high impact low frequency)	Regional SPS database

Information Attribute Examples			
Information Attribute	**Subcategory of Information**	**Purpose of Information Attribute**	**Possible Source(s)**
SCADA and EMS systems	EMS/GMS Systems and Vendors	To identify possible cyber gaps, CIP guidance, controls and monitoring and operational planning (if the Entity does not have power system analysis tools then ability to serve load is unknown). Possible risk is misplanning or causing an outage and identifying SOLs (N-1). Identify in-house design/vendor issues	Entity and Entity history
	Power system analysis tools		
	Network Diagrams		
	Authentication and Encryption		
	Operating Systems		
SCADA and EMS systems	Use of specialized automation used in the control system		
	Remote access capabilities		
	Physical security		
	System communication methods (e.g. copper, microwave, routable/non-routable, etc.)		
	ICCP systems		
Undervoltage load shedding		Potential risks in local system, awareness, control, system support/restoration/prevention. Very high risk facilities when called upon to protect against misoperation	PA study, Entity data submittals to REs and other Regional data,
Underfrequency load shedding		Potential risks in local system, awareness, control, system support/restoration/prevention. Very high risk facilities when called upon to protect against misoperation	PA study, Entity data submittals to REs and other Regional data
System restoration plan and responsibilities		Understanding Entity and responsibilities for how you restore system and reduce length of blackout	RC/TOP Plans, PA submittals to REs

Information Attribute Examples			
Information Attribute	**Subcategory of Information**	**Purpose of Information Attribute**	**Possible Source(s)**
Blackstart resources		Understanding Entity and responsibilities for how you restore system and reduce length of blackout	Regional Blackstart databased or Entity
IROLS		Understanding of potential operating risk for certain Entity's facilities	RC/TOP, PA, Entity
SOLS, Voltage SOLS, Stability SOLS		Understanding of potential operating risk for certain Entity's facilities	RC/TOP, Entity
Critical Facilities designated by Planning Authority		Understanding of potential operating risk for certain Entity's facilities	PA
CIP Critical Transmission and Generation Facilities		Understanding of potential operating risk for certain Entity's facilities	Entity and Regional Entity database
Generation Portfolio	Generator name	Magnitude of possible impact	Entity registration and system models
	Nameplate capacity		
	MVAR capability		
	Fuel type		
	Ownership		
	Compliance responsibilities		
Transmission portfolio	Transmission line mileage	Magnitude of possible impact	TADs for 200 kV and higher, Entity and system models for other
	Transmission line unique identifier	Magnitude of possible impact	TADs for 200 kV and higher, Entity and system models for other
	Line voltage	Magnitude of possible impact	TADs for 200 kV and higher, Entity and system models for other
	Compliance responsibilities	Awareness and Entity understanding of Entity footprint (asset ownership)	Entity
	Ownership and operation	Awareness and Entity understanding of Entity footprint (asset ownership)	Entity

Information Attribute Examples			
Information Attribute	**Subcategory of Information**	**Purpose of Information Attribute**	**Possible Source(s)**
Major changes to Entity's operations	Changes to transmission and generation portfolios (sales/acquisitions/retirements/replacements)	Magnitude of possible impact and potential changes in responsibilities	Public media, Entity, PA/BA
Regional Factors Affecting Reliability	System geography, climatology	Impact awareness	Public info
Compliance and Enforcement History	Self-reports: Number, types, ratio of self-reports versus violation history, Standards violated in Self-Reports	Understanding of Entity culture of compliance and potential areas of concern and possible IRA impacts.	Entity
Compliance and Enforcement History	Compliance activities: Involvement in TFEs, periodic data submittals, self-certifications, areas of concern and audit recommendations	Understanding of Entity culture of compliance and potential areas of concern and possible IRA impacts.	Entity
	Enforcement activities: Mitigation Plans and milestones, corrective actions, mitigation plan status that would impact further compliance activities	Understanding of Entity culture of compliance and potential areas of concern and possible IRA impacts	Entity
Events and Misoperations-operations History	Number/type of misoperations	Understand potential risk related to corrective action	Misoperations database, Entity reporting via TADS, GADS, DADS
	Root cause analysis/corrective action/compliance assessment	Understand potential risk related to corrective action	NERC/RE (RAPA, operations group) reports and information
	Event reports	Understand Entity operations and its high risk facility and interconnection information	RE
	Emergency Energy Alerts	To identify reoccurring issues that may impact reliable operations	RC
			NERC RCIS/CIPIS and ES-ISAC and OE-417

Appendix C – Risk Factor Examples

Possible Risk Factors		Possible Criteria for Assessment		
Risk Factor Example	**Risk Factor Subcategory**	**Low Risk**	**Medium Risk**	**High Risk**
System Geography	Geography	Entity has no areas of challenging system geography (rugged terrain, mountains, oceans, etc.)	Entity has a moderate amount of rugged terrain that impacts a moderate load of generation	Entity has a large amount of rugged terrain that impacts a large part of the bulk electric system
	Vegetation Management		Entity operates in a climate with moderate vegetation management issues	Entity operates in a climate with extremely invasive vegetation and has faced issues affecting vegetation management in the past
Peak Load and Capacity	Number of customers/NEL/critical customers	Entity provides service for less than 2% of the total region and no critical customers identified within the service area	Entity provides primary power supply for 10% - 20% of region	Entity provides primary power supply for 50%+ of region and/or provides power supply to major military bases, communication hubs, etc.
	Transmission Substation Voltage	No transmission	100kV-345kV	500KV+
	Total megawatt output (Generation)	<1000MW	1000MW - 5000MW	10000MW+
	Peak Load	<1000MW	1000 - 5000MW	10000MW+
BPS Exposure	Critical Facilities designated by Planning Authority	Entity has no critical facilities designated by PA		Entity has critical facilities designated by their PA
	Manual Load Shed	No manual load shed responsibilities	Responsible for dropping load during manual load shed.	Responsible for directing manual load shed.
BPS Exposure	Effective mix of power generating resources and percentage of their total megawatt output capability	Entity has a diverse array of power sources and can easily recover with changing conditions across the ERO (e.g. MATS)		Entity has a limited array of power sources and back up choices for power

Possible Risk Factors		Possible Criteria for Assessment		
Risk Factor Example	**Risk Factor Subcategory**	**Low Risk**	**Medium Risk**	**High Risk**
	Major Changes to entity's operations from:	Entity has not had any major changes to their organization	Entity has been purchased by an entity that has not previously been registered/with no previous compliance history	Entity has a negative compliance history and has been purchased by an entity with a negative compliance history.
	New and current service agreements (possibly JRO/CFR) with neighboring registered entities	Entity does not have any current service agreements	Entity has service agreements with entities without any previous history that has not previously been registered/with no previous compliance history	Entity and neighboring registered entities have service level agreements that have failed and caused outages
	Registered entity's current organizational reporting structure and upper management	Registered entity has an internal compliance function (depending on the size of the entity, this may be an internal compliance plan or program in the case of a smaller entity or it may be a separate department in the case of a larger entity) or other independent resource that reviews NERC Reliability Standards that is completely independent of NERC Reliability Standard performance	Registered entity has an internal compliance function (depending on the size of the entity, this may be an internal compliance plan or program in the case of a smaller entity or it may be a separate department in the case of a larger entity) that does not audit NERC Reliability Standards, but that is independent of NERC Reliability Standard performance and provides some level of oversight of the standards	Registered entity has limited or no formal internal compliance function. NERC Reliability Standards are done on an ad-hoc basis and there is some indication of failure of management oversight of NERC Reliability Standards
Interconnection points and critical paths/IROLs		Entity does not have any critical paths/IROLs on the BES	Entity has three or fewer critical paths/IROLs on the BES	Entity has 20+ critical path/IROLs on the BES

Possible Risk Factors		Possible Criteria for Assessment		
Risk Factor Example	**Risk Factor Subcategory**	**Low Risk**	**Medium Risk**	**High Risk**
Special Protection Systems, undervoltage load shedding, and underfrequency load shedding	SPS	Entity has no SPS	Entity has 1 SPS	Entity has 2 or more SPS and/or entity has a history of misoperations associated with any of their SPS
	Undervoltage load shedding	Entity has no UVLS capability	Entity has automated UVLS and has utilized this previously	Entity UVLS has caused widespread reliability issues
	Underfrequency load shedding	Entity has no UFLS capability	Entity has automated UFLS and has utilized this previously	Entity UFLS has caused widespread reliability issues
SCADA and EMS		Entity has no EMS or SCADA systems	Entity has an EMS/SCADA system that provides data and equipment control to RC/BA/TOP.	Entity has an EMS system that performs the RC and/or BA function, and has a history of issues.
System restoration responsibilities	General system restoration	Entity has no Regional or company system restoration responsibilities	Entity has black start units and/or provides switching other logistics for restoration plan.	Entity responsible for independent actions coordinated with the RC, or entity is an RC.
	Control Center Location(s)	Entity is in a low populated area and/or lo environmental exposure.	Entity is in moderately populated area with moderate crime rates and environmental exposure.	Entity is in highly populated area with high crime rates and/or high exposure to environmental disturbances. (e.g. Proximity to airport flight path and railway lines that carry hazardous material.)
System events and trends	Number of misoperations	Misoperations constitute less than 5% of all entity operations within the given time frame	Misoperations constitute between 5% and 15% of all entity operations within the given time frame	Misoperations constitute 20% or more of all entity operations within the given time frame

Possible Risk Factors		Possible Criteria for Assessment		
Risk Factor Example	**Risk Factor Subcategory**	**Low Risk**	**Medium Risk**	**High Risk**
	Misoperations resulting in event	Misoperations did not result in any event	Misoperation resulted in a Category 1 event or created conditions that could have resulted in a Category 1 event	Misoperations resulted in a Category 2 event or greater and/or included a cyber event that affected more than one entity
	Cause codes for multiple misoperations	Different causes/reasons for misoperations to demonstrate that entity manages misoperations root causes	Misoperations are a mix of different and repetitive cause codes, but where the same, entity demonstrates positive action in developing mitigation strategies/resolving issues	Repeated misoperations for same issue, demonstrating that entity is not able to develop mitigation strategies that improve system reliability
	How long did it take RE to mitigate the misoperation	RE completes mitigation plan in 15 days from misoperations and meets all milestones for resolution of misoperation	RE completes mitigation plan in 90 days from misoperations and meets all milestones for resolution of misoperation	RE takes 2+ years to mitigate misoperation and/or misses major milestones on mitigation plan to resolve misoperation
System events and trends	Registered Entity participation in root cause analysis	Entity voluntarily conducted compliance assessment for all events/misoperations and all cyber events	Entity conducted a compliance assessment for each Category 2 event and all cyber events	Entity did not conduct effective compliance assessments for their misoperations/events
Compliance history and trends	Self reporting process	Entity proactively identifies and self reports violations of NERC reliability standards. When a violation is discovered, Entity effectively identifies root cause of issue and does not violate the standard again.	Entity proactively identifies and self reports violations of NERC Reliability Standards, but does not always accurately assess the root cause of the violation, causing occasional repeat violations.	Entity does not identify issues with compliance with NERC Reliability Standards, and when violations are discovered, there is evidence that Entity works to cover up violation or avoid discovery.

Possible Risk Factors		Possible Criteria for Assessment		
Risk Factor Example	**Risk Factor Subcategory**	**Low Risk**	**Medium Risk**	**High Risk**
	Mitigation Plan Status	Entity regularly meets expectations of mitigation plans and hits all target deadlines.	Entity has met some, but not expectations of mitigation plans and milestones and may miss target deadlines.	Entity does not meet expectations of mitigation plans and misses most, if not all target deadlines.